Kit Izenpe

Instalación y manual de Usuario para Mac OS X

IZENPE
Beato Tomás de Zumarraga 71 - 1ª Planta
01008 Vitoria - Gasteiz
Tel.: 945 067 723
www.izenpe.com

Sumario

Introducción 3
A quién va dirigido este documento 3
Antes de comenzar 3
Instalación 4
Instalación controladores cryptoKEY 4
Instalación de Izenpe Middleware 7
Instalación manual de Izenpe Middleware 9
Problemas conocidos 10
Configuración en Firefox 10
Antes de comenzar a usar el Kit Izenpe 12
Uso de PIN Manager 13
Funcionalidades 13
Tabla de funciones 14
Preguntas frecuentes 16
Glosario 17

Introducción

Este manual sirve de guía para llevar a cabo de manera exitosa el proceso de instalación del Kit Izenpe, para el uso de las tarjetas criptográficas Izenpe (también para aquellas que vengan incorporadas en el token USB cryptoKEY), y el procedimiento para acceder y usar la aplicación de gestión. El Kit Izenpe consta de los siguientes componentes:

- **Izenpe Middleware**: librerías que permiten a cualquier aplicación del Sistema Operativo operar con las tarjetas criptográficas mencionadas
- **Izenpe PIN Manager**: aplicación para la gestión de la tarjeta, que permite realizar operaciones como cambio de PIN o PUK, desbloqueo de PIN, obtener información sobre la tarjeta,...
- **Controladores token cryptoKEY**: librerías para permitir al sistema operativo interactuar satisfactoriamente con el token USB cryptoKEY **(sólo en el caso que su tarjeta venga incorporada en un token USB cryptoKEY)**

Este manual le guiará de una manera sencilla en el proceso de instalación y uso del Kit Izenpe.

A quién va dirigido este documento

- ***Usuarios finales***, que desean utilizar la tarjeta con chip de Izenpe en entornos Mac OS X.

Antes de comenzar

Asegúrese de disponer de:

- Un lector de tarjetas estándar, compatible PC/SC que se encuentra correctamente conectado, instalado y configurado. Siga las instrucciones suministradas por el fabricante del lector para verificar su correcta instalación y funcionamiento **(en el caso de disponer de un token cryptoKEY no es necesario).**
- Disponer de la última versión del Kit Izenpe. Recomendamos visitar el sitio web de Izenpe para verificar que se trata de la versión actualizada.
- Si dispone de un token cryptoKEY asegúrese de tener la última versión de los controladores del token. Recomendamos visitar el sitio web de Izenpe para verificar que se trata de la versión actualizada.
- Para poder realizar la instalación, es indispensable poseer permisos de Administrador. En caso de no poseerlos la instalación será denegada.

En el caso de disponer de un token USB cryptoKEY de Bit4id no lo conecte a su ordenador hasta que no haya concluido la instalación.

Instalación

La aplicación estará accesible a través de la web de Izenpe, a través del apartado "Gestiona tu certificado" > Puesta en marcha de un Certificado

Descargue el instalador correspondiente a Mac OS X.

Instalación controladores cryptoKEY

Tras descargar el instalador, se debe descomprimir el archivo zip y empezar con la instalación de los drivers del lector, haciendo doble click sobre *bit4id-drivers.mpkg* **(este paso solo es necesario en caso de disponer de un token cryptoKEY).**

Se lanzará el instalador. Hacer click en *Continuar.*

En el siguiente paso, revisar las instrucciones de instalación y hacer click en *Continuar*.

A continuación, escoger la unidad de destino. Es importante permitir que se realice la instalación estándar en el disco principal.

Hacer click en continuar para lanzar la instalación.

Se solicitará acceso de administrador al equipo, dado que se van a instalar y configurar librerías de importancia.

Una vez concluida la instalación, reiniciar. Una vez concluido el reinicio, proceder con el siguiente paso.

Instalación de Izenpe Middleware

Hacer doble click sobre el icono del instalador, *Izenpe-middleware.pkg.dmg* para montar la unidad conteniendo el instalador*, Izenpe-middleware.pkg*

Se lanzará el instalador. Hacer click en *Continuar*.

En el siguiente paso, revisar las instrucciones de instalación y hacer click en *Continuar*.

ATENCIÓN: los tres idiomas disponibles Castellano, Euskera e Inglés se pueden revisar bajando la barra deslizante lateral.

Instalar Izenpe Middleware
Información importante
Introducción
Léame
Licencia
Selección de destino
Tipo de instalación
Instalación
Resumen
"Izenpe Middleware para Mac OS X"
"Mac OS X-entzako Izenpe Middleware "
"Izenpe Middleware for Mac OS X"
Castellano
Una vez completada la instalación, es necesario reiniciar el sistema.
Este software requiere un lector de tarjetas inteligentes compatible con el componente Apple Smartcard Services correctamente instalado y configurado en el sistema.
Este paquete instala el soporte para el navegador Safari. También instala la librería PKCS#11, para usar con programas como Mozilla Firefox.
La librería PKCS#11 se instalará en la siguiente ruta:
/System/Library/Izenpe/pkcs11/libbit4ipki.dylib
Para la instalación de la librería PKCS#11 en Mozilla
Imprimir...
Guardar...
Retroceder
Continuar

A continuación se presenta el acuerdo de licencia.

ATENCIÓN: los tres idiomas disponibles: Castellano, Euskera e Inglés se pueden revisar bajando la barra deslizante.

Instalar Izenpe Middleware
Contrato de licencia
Introducción
Léame
Licencia
Selección de destino
Tipo de instalación
Instalación
Resumen
CONTRATO DE LICENCIA DE USO DEL SOFTWARE MIDDLEWARE DE IZENPE
IZENPEREN MIDDLEWARE SOFTWAREA ERABILTZEKO LIZENTZIA KONTRATUA
LICENSE AGREEMENT FOR THE USE OF IZENPE MIDDLEWARE
- Si Ud. requiriese mayores informaciones sobre este Contrato de Licencia le rogamos que se dirija a IZENPE S.A. calle Beato Tomás de Zumárraga, 71, 1ª planta- 945067723- fax 945067709- info@izenpe.com. Cualquier cambio será debidamente anunciado en la página internet de IZENPE, www.izenpe.com.
CLAÚSULAS
Primera. Licencia de uso del software Middleware de IZENPE
A través de la presente licencia IZENPE concede al usuario el derecho de uso personal, no comercial, no exclusivo y no transferible de la copia del
Imprimir...
Guardar...
Retroceder
Continuar

Es necesario aceptar el acuerdo de licencia para continuar. Haga click en *Acepto*.

Para continuar con la instalación, debe aceptar las condiciones del contrato de licencia de software.
Haga clic en "Acepto" para continuar o en "No acepto" para cancelar la instalación y salir del Instalador.
Leer licencia
No acepto
Acepto

Es importante permitir que se realice la instalación estándar, en el directorio predeterminado, para simplificar la configuración. Hacer click en *Instalar*.

Se solicitará acceso de administrador al equipo, dado que se van a instalar y configurar librerías de importancia.

La instalación ha concluido con éxito:

En este momento puede conectar su token cryptoKEY de Bit4id a un puerto USB libre de su ordenador. Mac OS X lo reconocerá automáticamente, sin mostrar ningún mensaje por pantalla. El LED verde del dispositivo quedará fijo, indicando que la comunicación entre el token y el ordenador es satisfactoria, y todo funciona correctamente.

Instalación manual de Izenpe Middleware

En este punto se describe los pasos necesarios para la instalación manual, mediante la copia de las librerías en los directorios requeridos. El interfaz PKCS#11 de Izenpe Middleware para Mac OS X está constituido por dos archivos:

`libbit4ipki.dylib.conf`

`libbit4ipki.dylib`

Los dos archivos se copian siempre juntos en la misma carpeta de librerías que dependerá de la versión utilizada. Por ejemplo:

```
/System/Library/Izenpe/pkcs11
```

Problemas conocidos

La librería puede ser utilizada con Mozilla Firefox para una autenticación client SSL.

No obstante, un bug de Mozilla impide especificar la ruta de la librería utilizando la interfaz gráfica; de hecho podría suceder que después de haber seleccionado la librería, Firefox visualice una ruta del tipo:

AAAAAAFWAAIAAAxNYWNpbnRvc2ggSEQAAAAAAAAAAAAAAAAAAAC

Para evitar el problema, es necesario introducir manualmente la ruta completa de la librería en el campo en cuestión, por ejemplo:

```
/System/Library/Izenpe/pkcs11/libbit4ipki.dylib
```

Configuración en Firefox

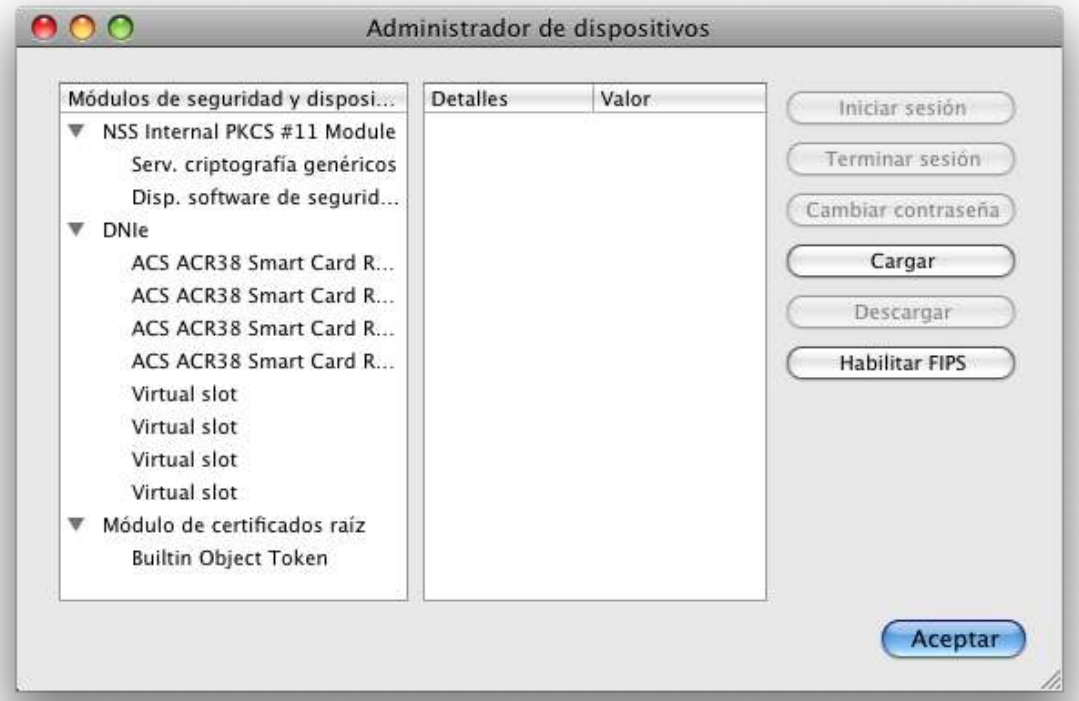
Para poder utilizar la tarjeta inteligente en el navegador Mozilla Firefox es necesario incorporar el soporte a las librerías del Universal Middleware de forma manual. Este procedimiento solo debe realizar si la instalación automatizada ha fallado.

Tras abrir Mozilla Firefox, se debe hacer click en *Firefox* → *Preferencias*

A continuación, seleccionar la pestaña *Cifrado* y hacer click en *Dispositivos de Seguridad*

Avanzado
General
Pestañas
Contenido
Aplicaciones
Privacidad
Seguridad
Avanzado
General
Red
Actualizar
Cifrado
Protocolos
Usar SSL 3.0
Usar TLS 1.0
Certificados
Cuando un servidor requiera mi certificado personal:
Seleccionar uno automáticamente
Preguntar siempre
Ver certificados
Listas de revocación
Validación
Dispositivos de seguridad

En la pantalla del *Administrador de dispositivos* de seguridad, hacer click en el botón *Cargar*.



En la ventana *Cargar dispositivo PKCS#11* se deben introducir los siguientes datos:

- Nombre del módulo: *Izenpe Middleware*
- Archivo del módulo: `/System/Library/Izenpe/pkcs11/libbit4ipki.dylib`

A continuación, hacer click en *Aceptar*. El módulo se incorporará satisfactoriamente, y la instalación en Firefox habrá concluido.

Antes de comenzar a usar el Kit Izenpe

Izenpe PIN Manager requiere un lector de tarjetas estándar, compatible PC/SC, que se encuentre correctamente conectado, instalado y configurado antes de comenzar.

Siga las instrucciones suministradas por el fabricante del lector para verificar su correcta instalación y funcionamiento.

En el caso de disponer de un token cryptoKEY asegúrese de tenerlo conectado en un puerto USB libre de su ordenador, y de que el token tiene una tarjeta inteligente (tamaño SIM) en su interior.

Uso de PIN Manager

La aplicación Izenpe PIN Manager está disponible dentro del menú Aplicaciones.

Funcionalidades

Izenpe PIN Manager dispone de múltiples funcionalidades, accesibles desde la pantalla principal:

[Imagen 1]

Tabla de funciones

La siguiente tabla resume las funciones expuestas en la pantalla principal de Izenpe PIN Manager.

Función	Descripción
Cambiar PIN	Función para cambiar el PIN de la tarjeta (ver imagen 2)
Desbloquear PIN	Función para desbloquear el PIN de la tarjeta mediante el PUK de la misma (ver imagen 3)
Cambiar PUK	Función para cambiar el PUK de la tarjeta (ver imagen 4)
Información de la tarjeta	Ventana que muestra información sobre la tarjeta (modelo, número de serie, identificación del fabricante y etiqueta) (ver imagen 5)

Cambiar PIN

Introduzca el PIN antiguo de la tarjeta y el nuevo PIN. El nuevo PIN tiene que tener entre 6 y 8 dígitos alfanuméricos.

[Imagen 2]

Desbloquear PIN

Para desbloquear el PIN, introduzca el PUK de la tarjeta e introducir el nuevo PIN. El nuevo PIN tiene que tener entre 6 y 8 dígitos alfanuméricos.

[Imagen 3]

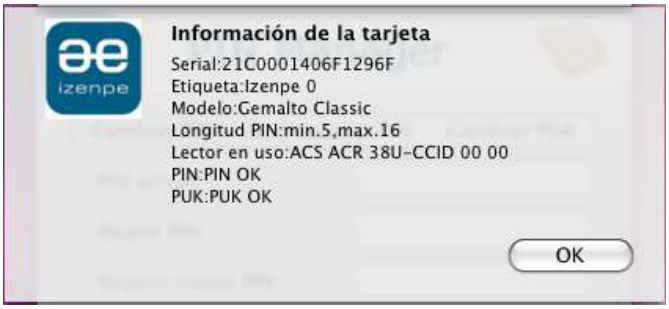
Cambiar PUK

Introduzca el PUK antiguo de la tarjeta y el nuevo PUK. El nuevo PUK tiene que tener entre 6 y 8 ígitos alfanuméricos.

[Imagen 4]

Información de la tarjeta

Ofrece información detallada de la tarjeta: modelo, número de serie, fabricante y etiqueta. Es posible que el CAU le solicite dicha información para conocer el tipo de tarjeta que está utilizando.



[Imagen 5]

Preguntas frecuentes

¿Qué puede ocurrir si tras haber instalado todas las aplicaciones y al conectar mi token cryptoKEY este no se ilumina con una luz verde?

Conecte el lector en otro puerto USB de otro ordenador. Si sigue sin funcionar, pruebe en otro ordenador. Si el LED verde nunca se ilumina, consulte con Izenpe para reemplazar el token cryptoKEY.

¿Cómo puedo comprobar que mi token cryptoKEY lleva incorporada una tarjeta inteligente tamaño SIM en su interior?

Abra la pestaña que se encuentra en el lado puerto al conector USB y verifique, según la foto adjunta, que tiene una tarjeta inteligente tamaño SIM en su interior, insertada correctamente.

¿Puedo combinar números y letras para el número PIN de la tarjeta?

Sí, no hay ningún problema, siempre que el nuevo PIN tenga entre 6 y 8 dígitos.

¿Existe un máximo de inserciones de PIN en el caso de que tenga alguna duda y no recuerde mi número PIN? ¿Cuándo puede quedar bloqueada la tarjeta?

Si inserta más de 3 veces el código PIN de forma errónea, este se bloquea. Póngase en contacto con Izenpe para desbloquearlo.

¿Existe un máximo de inserciones de PUK para intentar desbloquear el PIN? ¿Qué ocurre si la tarjeta queda bloqueada?

Si inserta más de 3 veces el código PUK de forma errónea, este se bloquea. Por razones de seguridad, la tarjeta se bloquea completamente. Póngase en contacto con Izenpe.

Glosario

Autoridad de Certificación: Es la entidad de confianza, responsable de emitir y revocar los certificados electrónicos, utilizados en la firma electrónica. La Autoridad de Certificación, por sí misma o mediante la intervención de una Autoridad de Registro, verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad.

Caducidad del certificado digital: El certificado digital tiene un período de vigencia que consta en el mismo certificado. Generalmente es de 2 años, aunque por ley se permite una vigencia de hasta 5 años. Una vez el certificado haya caducado, no se podrán utilizar los servicios ofrecidos por la Administración que requieran firma electrónica, y cualquier firma electrónica que se haga a partir de ese momento no tendrá validez.

Certificado digital: Documento en soporte informático emitido y firmado por la Autoridad de Certificación, que garantiza la identidad de su propietario.

Certificado reconocido: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone el capítulo II del Título II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Firma electrónica: Conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. Existen 3 tipos de firma electrónica: firma electrónica simple, avanzada y reconocida.

Firma electrónica simple: Conjunto de datos, en forma electrónica, anejos a otros datos.

Firma electrónica avanzada: Firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Firma electrónica reconocida: Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Función hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.

Hash o Huella digital: Resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

Integridad: La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

Listas de Revocación de Certificados o Listas de Certificados Revocados: Lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

No repudio: El emisor que firme electrónicamente un documento no podrá negar que envió el mensaje original, ya que éste es imputable al emisor por medio de la clave privada que únicamente conoce él y que está obligado a custodiar. El no repudio permite, además, comprobar quién participó en una transacción.

El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero

Prestador de Servicios de Certificación o PSC: Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. Ver Autoridad de Certificación.

PIN: Secuencia de caracteres que permiten el acceso a los certificados. Número de Identificación Personal, en ocasiones llamado NIP.

PUK: Secuencia de caracteres que permiten el cambio o desbloqueo del PIN. Clave Personal de Desbloqueo.

Renovación: La renovación consiste en solicitar un nuevo certificado mediante un certificado vigente pero que está a punto de caducar. De esta manera, antes de la caducidad de un certificado se puede solicitar la renovación y esto implica que se emita un nuevo certificado válido.

Revocación: Anulación definitiva de un certificado digital a petición del suscriptor, o por propia iniciativa de la Autoridad de Certificación en caso de duda de la seguridad de las claves. La

revocación es un estado irreversible. Se puede solicitar la revocación de un certificado después de una situación de suspensión o por voluntad de las personas autorizadas a solicitarla. De la misma manera, en el caso de un certificado suspendido, si ha pasado el periodo de suspensión máximo, si el certificado no ha sido habilitado, pasa a estar definitivamente revocado. Cuando la entidad de certificación revoca o suspende un certificado, ha de hacerlo constar en las Listas de Certificados Revocados (CRL), para hacer público este hecho. Estas listas son públicas y deben estar siempre disponibles.

Tarjeta inteligente (smartcard): Cualquier tarjeta con circuitos integrados que permiten la ejecución de cierta lógica programada.